

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

BO-HEUNG CHUNG, ET AL.

Application No.:

Filed:

For: **METHOD FOR DYNAMICALLY
CHANGING INTRUSION DETECTION
RULE IN KERNEL LEVEL INTRUSION
DETECTION SYSTEM**

Art Group:

Examiner:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR PRIORITY

Sir:

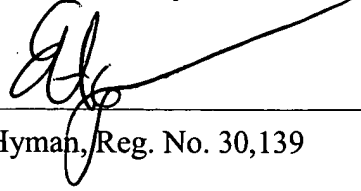
Applicant respectfully requests a convention priority for the above-captioned application, namely:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>DATE OF FILING</u>
Korea	10-2003-0079581	11 November 2003

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP



Eric S. Hyman, Reg. No. 30,139

Dated: December 29, 2003

12400 Wilshire Boulevard, 7th Floor
Los Angeles, CA 90025
Telephone: (310) 207-3800



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Intellectual
Property Office.

출원 번호 : 10-2003-0079581
Application Number

출원 년 월 일 : 2003년 11월 11일
Date of Application NOV 11, 2003

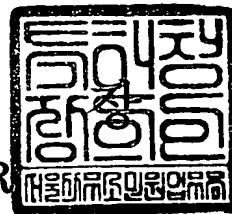
출원인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Inst



2003 년 11 월 28 일

특 허 청

COMMISSIONER



【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2003.11.11
【발명의 명칭】	커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법
【발명의 영문명칭】	Dynamic Changing Method of Intrusion Detection Rule In Kernel Level Intrusion Detection System
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【명칭】	특허법인 신성
【대리인코드】	9-2000-100004-8
【지정된변리사】	변리사 정지원, 변리사 원석희, 변리사 박해천
【포괄위임등록번호】	2000-051975-8
【발명자】	
【성명의 국문표기】	정보흥
【성명의 영문표기】	CHUNG, Bo Heung
【주민등록번호】	700904-1024912
【우편번호】	305-308
【주소】	대전광역시 유성구 장대동 359-2 402호
【국적】	KR
【발명자】	
【성명의 국문표기】	류승호
【성명의 영문표기】	RYU, Seung Ho
【주민등록번호】	751028-1696411
【우편번호】	305-350
【주소】	대전광역시 유성구 가정동 236-1 ETRI 기숙사 312호
【국적】	KR
【발명자】	
【성명의 국문표기】	김정녀
【성명의 영문표기】	KIM, Jeong Nyeo

【주민등록번호】	650919-2565712
【우편번호】	302-181
【주소】	대전광역시 서구 내동 코오롱아파트 8-801
【국적】	KR
【발명자】	
【성명의 국문표기】	손승원
【성명의 영문표기】	SOHN, Sung Won
【주민등록번호】	571225-1674514
【우편번호】	305-390
【주소】	대전광역시 유성구 전민동 엑스포아파트 208-902
【국적】	KR
【발명자】	
【성명의 국문표기】	박치항
【성명의 영문표기】	PARK, Chee Hang
【주민등록번호】	470112-1069516
【우편번호】	305-333
【주소】	대전광역시 유성구 어은동 한빛아파트 131-1002
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인 특허법인 신성 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	5 면 5,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	5 항 269,000 원
【합계】	303,000 원
【감면사유】	정부출연연구기관
【감면후 수수료】	151,500 원
【기술이전】	
【기술양도】	희망
【실시권 허여】	희망
【기술지도】	희망

1020030079581

출력 일자: 2003/12/4

【첨부서류】

1. 요약서·명세서(도면)_1통

【요약서】**【요약】****1. 청구범위에 기재된 발명이 속하는 기술분야**

본 발명은, 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법 에 관한 것
임.

2. 발명이 해결하려고 하는 기술적 과제

본 발명은, 커널 내에서 침입탐지 과정에 이용되는 침입탐지규칙의 복사본을 동적으로
관리하여, 사용자(User) 영역으로부터의 침입탐지규칙 변경 요청에 따라 먼저 상기 복사본에
대하여 변경 작업을 수행한 후, 현재 적용중인 침입탐지규칙과 교체(포인터 교환)함으로써, 침
입탐지규칙의 변경시에도 침입탐지 과정의 연속성을 보장하기 위한, 커널 기반의 침입탐지시스
템에서의 침입탐지규칙 동적 변경 방법을 제공하는데 그 목적이 있음.

3. 발명의 해결 방법의 요지

본 발명은, 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 관리 방법에 있어서,
커널 영역에서 침입탐지규칙의 복사본을 생성하는 제 1 단계; 사용자 영역으로부터의 침입탐지
규칙의 변경 요청에 따라 상기 침입탐지규칙의 복사본을 변경하는 제 2 단계; 및 상기 침입탐
지규칙을 가리키는 포인터의 값과 상기 변경된 침입탐지규칙의 복사본을 가리키는 포인터의 값
을 서로 교환하여 현재 적용중인 침입탐지규칙을 변경하는 제 3 단계를 포함함.

4. 발명의 중요한 용도

본 발명은 침입탐지시스템 등에 이용됨.

【대표도】

도 3

【색인어】

침입탐지시스템, 커널 기반, 침입탐지규칙 동적 변경, 전역변수, 복사본

【명세서】**【발명의 명칭】**

커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법 {Dynamic Changing Method of Intrusion Detection Rule In Kernel Level Intrusion Detection System}

【도면의 간단한 설명】

도 1은 본 발명이 적용되는 커널 기반의 침입탐지시스템의 일실시에 구성도.

도 2는 본 발명에 따른 커널 기반의 침입탐지시스템에서의 침입탐지규칙 변경 방법에 대한 일실시에 설명도.

도 3은 본 발명에 따른 커널 기반의 침입탐지시스템에서의 침입탐지규칙 변경 과정에 대한 일실시에 흐름도.

도 4는 본 발명에 따른 커널 기반의 침입탐지시스템에서의 침입탐지 과정에 대한 일실시에 흐름도.

* 도면의 주요 부분에 대한 부호 설명

11 : 침입탐지부 12 : 패킷처리부

13 : 네트워크 드라이버

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <8> 본 발명은, 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법에 관한 것이다.
- <9> 본 발명에서 침입탐지규칙 관리란 침입탐지규칙의 설정/해제/변경 등을 모두 포함하는 개념의 용어이다. 그 중에서 침입탐지규칙 변경 방법이 본 발명의 대상이다.
- <10> 일반적으로 침입탐지시스템(IDS : Intrusion Detection System)은 방화벽(fire wall)과 같은 단순한 접근 제어 기능을 넘어서서 침입의 패턴 데이터베이스와 전문가 시스템(Expert System)을 이용하여 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다.
- <11> 일반적으로 침입탐지시스템은 모니터링의 대상에 따라 네트워크를 기반으로 하는 시스템과 호스트(컴퓨터)를 기반으로 하는 시스템으로 나뉘어진다. 먼저, 호스트 침입탐지시스템은 시스템마다 침입탐지모듈이 설치되며, 로그데이터를 이용하여 하나의 시스템 내부 사용자들의 활동을 감시하고 해킹 시도를 탐지해낸다. 반면에, 네트워크 침입탐지시스템은 네트워크를 단위로 하나의 침입탐지모듈이 설치되며, 네트워크 패킷 캡처링을 기반으로 한 패킷 분석을 이용하여 침입을 탐지해낸다.
- <12> 최근에는 네트워크 환경 및 인터넷의 발달로 인하여 컴퓨터의 연결성과 사용자가 급속하게 증가하면서 네트워크를 통한 공격 및 침입을 효과적으로 탐지하여 네트워크 보안을 향상시키기 위한 분산 침입탐지시스템에 대한 필요성이 증가되고 있다.

- <13> 한편, 최근들어 복합적이고 다양한 네트워크 공격을 탐지하기 위하여 연구되고 있는 소프트웨어 에이전트 및 멀티 센서 기반의 네트워크 침입탐지시스템은 대량의 패킷이 네트워크로 전파되는 분산 서비스 거부 공격, 인터넷 웜과 같은 공격에 대하여서는 효율적이지 못하다. 왜냐하면, 일반적으로 소프트웨어 에이전트 및 멀티 센서 기반의 네트워크 침입탐지시스템은 네트워크를 통하여 전달받은 패킷을 커널에서 복사한 후 에이전트 또는 센서로 전달하기 때문에, 드롭되는 패킷들이 다수 발생하게 된다. 또한, 이와 같은 응용 프로그램 기반의 침입탐지 기술은 패킷 캡처 라이브러리 등을 이용하여 커널에서 복사된 패킷 데이터를 응용 프로그램으로 전달하는 과정에서 부하가 발생한다는 문제점을 가지고 있다.
- <14> 이러한 문제점을 해결하기 위한 종래의 기술로서 "리눅스 커널기반의 실시간 침입탐지시스템(Real-time Intrusion Detection System based Linux Kernel)"이 대한민국 특허 출원번호 제10-2002-0091340호에 개시되어 있다.
- <15> 상기 특허 출원 제10-2002-0091340호는, 상기와 같은 문제점을 해결하기 위하여, 종래의 침입탐지 기술을 바탕으로 커널을 수정하여 침입탐지를 수행하고, 감시 프로그램인 데몬 프로그램을 추가로 작성하여 보완하는 실시간 커널기반 침입탐지 기술을 이용하고 있다. 즉, 상기 특허 출원 제10-2002-0091340호는 컴퓨터 프로그램이 수행되는 시점에서 작업환경에 대한 정보를 획득하여 저장하도록 커널을 수정하고, 일종의 감시 프로그램인 데몬(Daemon) 프로그램에서 커널이 저장한 정보를 이용하여 작업을 수행시킨 사용자의 위치, 프로그램의 수행계통, 작업의 적법성 유무를 판단한 후, 그 결과를 콘솔(console)과 침입감시제어장치, 전자우편, 관리자 이동통신단말기 등으로 알리는 방법이다.
- <16> 그런데, 상기와 같은 종래의 실시간 커널기반 침입탐지 기술은 다음과 같은 문제점을 가지고 있다.

- <17> 첫째, 종래의 실시간 커널기반 침입탐지 기술은 급변하는 해킹 및 네트워크 공격에 대응하기 위한 효과적인 침입탐지규칙 변경 방법을 제공하지 못한다. 즉, 종래의 실시간 커널기반 침입탐지 기술은 침입탐지규칙이 변경되었을 경우에 커널을 수정하거나 재부팅시키는 작업이 필요하여, 침입탐지를 위한 커널의 연속성을 보장하기 어렵다는 문제점을 가진다. 따라서, 새로운 해킹 및 공격에 대한 적응력이 저하되고, 효과적인 침입방지와 네트워크 보안에 심각한 위협요소가 될 수 있다.
- <18> 둘째, 종래의 실시간 커널기반 침입탐지 기술은 커널 내에서의 효과적인 침입탐지규칙 관리 방법을 제공하지 못한다. 특히, 커널 메모리에서 관리되는 침입탐지규칙은 침입탐지 과정과 침입탐지규칙 변경 과정이 동시에 발생할 수 있기 때문에 커널 내 침입탐지 과정에 방해를 주지않으면서 커널 내 침입탐지규칙을 변경할 수 있도록 하는 효과적인 침입탐지규칙 변경 방법이 필요하다.
- <19> 셋째, 종래의 실시간 커널기반 침입탐지 기술은 탐지된 결과를 커널이 동작하고 있는 호스트의 데몬 프로그램으로 전달하는 방법만을 제공한다. 즉, 현재와 같은 분산 네트워크 환경에서 확장성과 보안관리시스템과의 연동을 위해서는 탐지된 결과를 최소한의 부하로 타 네트워크 또는 타 호스트(서버)로 전달할 수 있어야 한다. 그런데, 종래의 기술은 커널 내 탐지 결과를 응용 프로그램에 전달하고 다시 응용 프로그램에서 커널을 통하여 타 시스템으로 전달하는 과정을 사용하기 때문에 매우 비효율적이다.
- <20> 따라서, 커널 내 침입탐지 과정의 연속성을 보장하는 침입탐지규칙 변경 방법과 효과적인 침입탐지규칙 관리 방법, 그리고 분산 네트워크 환경에서의 확장성과 보안관리시스템과의 연동을 제공하는 실시간 커널기반 침입탐지 기술이 절실히 요구된다.

【발명이 이루고자 하는 기술적 과제】

- <21> 본 발명은, 상기와 같은 문제점을 해결하기 위하여 제안된 것으로, 커널 내에서 침입탐지 과정에 이용되는 침입탐지규칙의 복사본을 동적으로 관리하여, 사용자(User) 영역으로부터의 침입탐지규칙 변경 요청에 따라 먼저 상기 복사본에 대하여 변경 작업을 수행한 후, 현재 적용중인 침입탐지규칙과 교체(포인터 교환)함으로써, 침입탐지규칙의 변경시에도 침입탐지 과정의 연속성을 보장하기 위한, 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법을 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

- <22> 상기의 목적을 달성하기 위한 본 발명은, 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 관리 방법에 있어서, 커널 영역에서 침입탐지규칙의 복사본을 생성하는 제 1 단계; 사용자 영역으로부터의 침입탐지규칙의 변경 요청에 따라 상기 침입탐지규칙의 복사본을 변경하는 제 2 단계; 및 상기 침입탐지규칙을 가리키는 포인터의 값과 상기 변경된 침입탐지규칙의 복사본을 가리키는 포인터의 값을 서로 교환하여 현재 적용중인 침입탐지규칙을 변경하는 제 3 단계를 포함한다.
- <23> 또한, 상기 본 발명은, 상기 침입탐지규칙의 복사본을 현재 적용중인 침입탐지규칙과 동일하게 재변경하는 제 4 단계를 더 포함한다.
- <24> 상술한 목적, 특징들 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

- <25> 도 1은 본 발명이 적용되는 커널 기반의 침입탐지시스템의 일실시에 구성도이다.
- <26> 도 1에 도시된 바와 같이, 본 발명이 적용되는 커널 기반의 침입탐지시스템은, 크게 사용자(User) 영역과 커널(Kernel) 영역으로 나뉘어진다.
- <27> 먼저, 사용자(User) 영역의 응용 프로그램(14,15)은 커널 내의 침입탐지부(11)와의 인터페이스를 위하여 시스템 관리자 또는 보안관리자의 사용도구(사용자 응용 프로그램)를 확장한 것이라고 볼 수 있다.
- <28> 사용자 응용 프로그램(15,14)은 커널 내의 침입탐지부(11)로부터 침입탐지결과를 전달받아 처리하는 기능과 시스템 호출을 이용하여 침입탐지규칙에 대한 설정/해제/변경 등의 요청을 침입탐지부(11)로 전달하는 기능을 각각 수행한다. 이 때, 시스템 호출과 다른 방법으로서 "/proc/ids"에 "out_forwarding"과 IP 값을 설정하여, 침입탐지결과를 전달할 위치를 설정할 수 있다. 즉, 시스템 관리자 또는 보안관리자가 일반적인 "vi"와 같은 문서편집기를 이용하여 "/proc" 디렉토리의 "ids" 파일을 오픈한 후, "out_forwarding"과 IP 값을 변경하면 커널 내 침입탐지부(11)에서 이를 적용하여 침입탐지결과를 전달한다. 이 때, "/proc/ids" 파일은 시스템 관리자 또는 보안관리자만이 변경할 수 있고 그외의 권한을 가진 사용자는 이 작업을 수행할 수 없다.
- <29> 사용자 응용 프로그램(15)은 커널 내의 침입탐지부(11)로부터 전달받은 침입탐지결과를 사용자(User) 영역에서 실행되는 보안정책관리 프로그램, 그래픽 유저 인터페이스(GUI) 프로그램 또는 관리자 콘솔 등과 같은 프로그램에 전달하여 시스템 관리자 또는 보안관리자가 침입탐지결과에 대해 분석하고 새로운 침입탐지규칙을 생성하는데 이용하도록 한다.

- <30> 또한, 사용자 응용 프로그램(14)은 시스템 호출을 이용하여 침입탐지규칙에 대한 설정/해제/변경 등을 커널 내의 침입탐지부(11)에 요청하여, 커널이 침입탐지과정을 연속적으로 수행하면서 침입탐지규칙을 변경할 수 있도록 지원한다. 이로 인해, 커널을 다시 리부팅(rebooting)하지 않고도 새로운 침입탐지규칙을 적용할 수 있게 된다.
- <31> 한편, 커널(Kernel) 영역에서는 침입탐지 자료구조를 이용하여 네트워크 패킷에 대한 침입탐지 과정을 수행하며, 탐지된 결과를 사용자 영역의 응용 프로그램(분석모듈)으로 전송하여 사용자(User) 영역의 응용 프로그램(14,15)이 탐지된 결과를 이용하여 분석을 수행하거나 침입탐지 규칙에 대한 변환/변경 요청 처리 등을 수행하도록 한다.
- <32> 한편, 본 발명이 적용되는 커널 기반 침입탐지시스템의 커널(Kernel) 영역은 네트워크 드라이버(13), 패킷처리부(12), 및 침입탐지부(11)를 포함한다. 이 때, 네트워크 드라이버(13)와 패킷처리부(12)는 커널에서 기본적으로 제공되는 모듈이고, 침입탐지부(11)는 본 발명을 실행하기 위하여 필요한 모듈이다.
- <33> 먼저, 네트워크 드라이버(13)는 커널에서 기본적으로 제공되는 구성요소로서, 패킷에 대한 처리를 수행한다. 즉, 네트워크를 통해 전달되는 패킷들 중에서 자신의 IP 주소에 해당하는 패킷들은 패킷처리부(12)로 전달하고 그렇지 않은 패킷들은 그냥 통과시키는 기능을 한다. 또한, 사용자 응용 프로그램이나 커널의 다른 모듈로부터 패킷을 네트워크로 전달하라는 요청을 받으면 이들 패킷들을 네트워크로 전송하는 기능을 수행한다.
- <34> 그리고, 패킷처리부(12)는 네트워크 드라이버(13)를 통하여 전달받은 패킷을 침입탐지부(11)로 전달하는 역할을 수행하고, 침입탐지부(11)로부터 전달받은 패킷을 네트워크 드라이버(13)로 전달하는 기능을 수행한다. 패킷처리부(12)는 대개 커널에 구현된 전송제어프로토콜/인터넷프로토콜(TCP/IP) 스택 구현코드인 경우가 대부분이기 때문에 커널에서 기본적으로 제공되

는 구성요소로 볼 수 있으며, 패킷에 대한 소스(Source) IP/포트(Port), 목적지(Destination) IP/포트(Port)를 검사하여 패킷들을 필터링하는 기능(방화벽의 일부기능)을 수행하도록 구현할 수도 있다.

<35> 한편, 침입탐지부(11)는 침입탐지를 수행하는 기능과 침입탐지규칙들을 관리하는 기능을 수행한다. 먼저, 침입탐지기능은 패킷처리부(12)를 통하여 패킷이 도착할 때마다 미리 설정된 침입탐지규칙에 해당하는 패킷이 있는지 없는지를 검사하고 해당하는 패킷이 있으면 이를 사용자 응용 프로그램이나 외부 호스트에 있는 관리 서버로 전달하는 기능을 수행한다. 이 때, 기본적으로 침입탐지 결과는 사용자 응용 프로그램으로 전달되나 시스템 관리자 또는 보안관리자에 의해 외부의 관리 서버로 전달하도록 설정(/proc/ids)된 경우에는 해당 서버로 전달된다.

<36> 그리고, 침입탐지규칙 관리 기능은 침입탐지 수행시 사용할 침입탐지규칙을 커널에 설정/해제/변경하는 기능을 수행한다. 즉, 시스템 관리자 또는 보안관리자가 사용자(User) 영역에서 동작하는 사용자 응용 프로그램(14)을 통하여 커널 내의 침입탐지부(11)에 침입탐지규칙의 설정/해제/변경 등을 요청하고, 커널 내의 침입탐지부(11)는 응용 프로그램(14)으로부터의 요청에 따라 침입탐지규칙의 설정/해제/변경 등을 수행한다. 이러한 침입탐지규칙의 설정/해제/변경 요청은 사용자 응용프로그램이 커널에서 제공하는 시스템호출함수를 이용하여 커널로 전달하는 방식을 사용하며, 이를 위하여 커널에 기본적으로 제공되는 시스템호출함수를 확장한다.

<37> 이상에서 설명한 각 구성요소의 기능들을 요약하여 네트워크상의 패킷에 대한 침입탐지 과정과 침입탐지규칙에 대한 관리 과정을 간략히 설명하면 다음과 같다.

<38> 먼저, 침입탐지 과정을 살펴보면, 네트워크 드라이버(13)를 통하여 네트워크 상의 패킷이 입력되면, 입력된 패킷은 패킷처리부(12)로 전달되고, 패킷처리부(12)

에서 전송제어프로토콜/인터넷프로토콜(TCP/IP) 스택에서 정의된 기본적인 기능(패킷헤더 이상 유무 검사 등)을 수행한 후, 침입탐지부(11)로 전달한다. 그러면, 침입탐지부(11)에서는 침입 탐지규칙을 이용하여 전달받은 패킷에 대한 침입탐지 과정을 수행하며, 침입이 발견되면 그 결과를 사용자(User) 영역의 사용자 응용 프로그램(15) 또는 미리 설정된 외부 호스트에 존재하는 관리서버로 전달한다.

<39> 한편, 침입탐지규칙 관리(설정/해제/변경) 과정은 시스템 관리자 또는 보안관리자가 앞에서 설명한 관리자 콘솔, 그래픽 유저 인터페이스(GUI) 등을 이용하여 사용자 응용 프로그램(14)으로 침입탐지규칙에 대한 설정/해제/변경 등을 요청하고, 사용자 응용 프로그램(14,15)이 시스템 호출함수를 이용하여 침입탐지규칙 설정/해제/변경 요청을 침입탐지부(11)로 전달한다. 그러면, 침입탐지부(11)는 침입탐지규칙 설정/해제/변경 요청에 따라 침입탐지규칙을 설정/해제/변경하게 된다.

<40> 이와 같이, 본 발명이 적용되는 커널 기반의 침입탐지시스템은 침입탐지 과정과 침입분석 과정이 분리될 수 있으므로, 탐지/분석 모듈을 하나의 시스템이 아닌 서로 다른 시스템에서 운영할 수도 있고, 다수의 탐지모듈을 분산된 다수의 시스템에서 운영할 수도 있는 매우 유연한 구조를 가질 수 있다. 또한, 탐지과정이 커널(Kernel) 영역에서 동작하게 되기 때문에 사용자(User) 영역의 프로그램을 이용할 때보다 빠른 탐지속도를 보장할 수 있는 장점을 가지게 된다.

<41> 구체적인 침입탐지규칙 변경 과정 및 침입탐지 과정에 대하여서는 도 2 내지 도 4를 참조하여 상세히 살펴보기로 한다.

<42> 도 2는 본 발명에 따른 커널 기반의 침입탐지시스템에서의 침입탐지규칙 변경 방법에 대한 일실시에 설명도이다.

- <43> 도 2에 도시된 바와 같이, 본 발명에 따른 커널 기반의 침입탐지시스템에서 침입탐지규칙을 변경하는 방법은 크게 6 과정으로 진행되며, 이들 자료구조는 모두 커널 메모리에서 처리된다.
- <44> 먼저, "Curr"는 현재 침입탐지과정에서 사용되는 침입탐지규칙을 가리키는 포인터이고, "New"는 현재 침입탐지규칙에 대한 복사본을 가리키는 포인터로서, 침입탐지규칙 변경시에 이용된다. 또한, 침입탐지규칙 변경에 대한 상태를 나타내기 위하여 "Update", "Changing", "Changed"라는 커널 내 전역변수를 추가하여 사용한다.
- <45> 제 1 과정은 커널 내에 초기 침입탐지규칙이 설정된 상태를 나타낸다. "Curr"는 규칙 1(rule1)을 가리키고 있으며, "New"는 규칙1(rule1)에 대한 복사본을 가리키고 있다. 또한, 전역변수(Update, Changing, Changed)는 0으로 초기화된 상태이다.
- <46> 제 2 과정은 현재 적용중인 침입탐지규칙에 대한 변경 요구가 발생하였을 경우를 나타낸다. 이 때, "Curr"는 현재 침입탐지 과정에서 사용되고 있으므로 "New"가 가리키는 규칙 1(rule1)을 규칙2(rule2)로 변경하는 과정을 수행한다. 그리고, 전역변수 "Update" 및 "Changing"을 1로 설정하여 현재 침입탐지규칙의 변경이 진행되고 있음을 표시해준다.
- <47> 제 3 과정은 침입탐지규칙 변경이 완료된 상태를 나타내는 것으로서, 전역변수 "Changing"을 0으로 "Changed"를 1로 각각 설정하여 복사본(New)에 대한 침입탐지규칙의 변경이 완료되었음을 나타낸다.
- <48> 제 4 과정은 "Curr"와 "New"가 가리키는 포인터를 서로 교체하여 현재 침입탐지규칙을 새롭게 변경한 상태를 나타낸다. 이후로는 새로 변경된 침입탐지규칙을 이용하여 침입탐지를 수

행할 수 있게 된다. 이 때, 전역변수 "Changed"를 0으로 설정하여 현재 침입탐지규칙이 변경된 상태임을 나타낸다.

- <49> 제 5 과정은 현재 "Curr"가 가리키는 침입탐지규칙과 "New"가 가리키는 침입탐지규칙이 동일하지 않으므로, 이를 일치시키기 위하여 규칙1(rule1)을 규칙2(rule2)로 변경하는 과정을 수행한다.
- <50> 제 6 과정은 모든 침입탐지규칙 변경 과정이 완료된 상태로서, "Curr"가 가리키는 침입탐지규칙과 "New"가 가리키는 침입탐지규칙이 동일한 내용을 가지게 되었으므로, 전역변수 "Update"를 0으로 설정한다.
- <51> 상기와 같은 과정을 통하여서 커널 내에서 침입탐지 과정을 중단시키지 않고 침입탐지규칙 변경이 가능하게 되어, 침입탐지의 연속성을 보장할 수 있게 된다.
- <52> 도 3은 본 발명에 따른 커널 기반의 침입탐지시스템에서의 침입탐지규칙 변경 과정에 대한 일실시에 흐름도이다.
- <53> 먼저, 침입탐지부(11)가 사용자(User) 영역의 응용 프로그램으로부터 탐지규칙변경을 요청받으면(301) 전역변수 "Update" 값이 0인지를 확인한다(302).
- <54> 상기 확인 결과(302), "Update"의 값이 1이면 현재 침입탐지규칙 변경 과정 실행중에 있으므로, 사용자 영역의 응용 프로그램에 이를 알린 후, 종료한다.
- <55> 한편, 상기 확인 결과(302), "Update" 값이 0이면 전역변수 "Update" 및 "Changing"의 값을 1로 설정하고(303), "New" 포인터가 가리키는 침입탐지규칙을 새로운 침입탐지규칙으로 변경한다(304). 그리고, "New" 포인터가 가리키는 침입탐지규칙의 변경이 완료되면 전역변수 "Changing"의 값을 0으로 설정하고, "Changed"의 값을 1로 설정한다(305).

- <56> 이후, 전역변수 "Changed"의 값이 0으로 변환되었는지를 확인하여(306), 전역변수 "Changed"의 값이 0으로 변환되지 않았으면, "Curr" 포인터가 가리키는 침입탐지규칙이 아직 변경되지 않은 것이므로 일정시간 경과 후 "Changed"의 값을 재확인하게 된다. 이 때, 실제로 침입탐지에 이용되는 침입탐지규칙의 변경은, 즉 "Curr" 포인터가 가리키는 침입탐지규칙의 변경은 침입탐지를 수행하는 과정 중에 이루어진다. 이 과정에 대하여서는 도 4를 참조하여 후술하기로 한다.
- <57> 한편, 상기 확인 결과(306), 전역변수 "Changed"의 값이 0으로 변환되었으면 "New" 포인터가 가리키는 침입탐지규칙을 "Curr" 포인터가 가리키는 침입탐지규칙으로 재변경하여, "Curr"와 "New"가 가리키는 침입탐지규칙의 내용이 동일하도록 하고(307), 전역변수 "Update"의 값을 0으로 설정하여 침입탐지규칙 변경 과정이 모두 완료되었음을 알린다(308).
- <58> 도 4는 본 발명에 따른 커널 기반의 침입탐지시스템에서의 침입탐지 과정에 대한 일실시예 흐름도이다.
- <59> 먼저, 침입탐지부(11)가 네트워크 드라이버(13)를 통하여 패킷을 입력받으면(401), 전역변수 "Changing"의 값이 0인지를 확인하여(402), "Changing"의 값이 0이면 전역변수 "Changed"의 값이 1인지를 확인하여(403), "Changed"의 값이 1이면 "Curr" 포인터와 "New" 포인터가 가리키는 값을 서로 교체하여 현재 적용되는 침입탐지규칙을 변경하고(404), 전역변수 "Changed"의 값을 0으로 설정한다(405). 그리고, "Curr" 포인터가 가리키는 침입탐지규칙을 이용하여 침입탐지 과정을 수행한다(406). 이 때, 침입탐지 과정에 이용되는 침입탐지규칙은 새롭게 변경된 침입탐지규칙이 된다.

- <60> 한편, 상기 확인 결과(402, 403), 전역변수 "Changing"의 값이 1이거나, "Changed"의 값이 0이면 "406"과정으로 진행하여, 현재 "Curr" 포인터가 가리키는 침입탐지규칙을 이용하여 침입탐지 과정을 수행한다. 이때, 침입탐지 과정에 이용되는 침입탐지규칙은 변경되지 않은(또는 이전에 변경된) 침입탐지규칙이 된다.
- <61> 상기와 같은 침입탐지 과정은 침입탐지규칙 변경 과정과는 별개로 동작하며, 항상 현재의 "Curr" 포인터가 가리키는 침입탐지규칙을 이용하기 때문에, 침입탐지의 연속성을 보장할 수 있게 된다. 왜냐하면, 침입탐지의 관점에서 보면 "Curr" 포인터의 값과 "New" 포인터의 값을 서로 교환하는 단순한 과정에 의하여 침입탐지규칙이 변경되기 때문이다.
- <62> 한편, 상기와 같은 침입탐지 과정을 통하여 커널 내에서 탐지된 침입탐지 결과는 캐릭터 디바이스 등을 통하여 사용자(User) 영역의 응용 프로그램으로 전달된다. 또한, 원격지에 존재하는 침입분석 및 보안관리 서버로 침입탐지 결과를 전달하기 위해서는 커널 내의 포워딩 로직을 이용하여 전달한다.
- <63> 이상에서 살펴본 바와 같이, 본 발명은 커널 내에서 침입탐지를 수행하고, 패킷 필터링과 침입 분석을 응용 프로그램 영역이 아닌 커널 영역에서 제공함으로써, 침입탐지를 최적화할 수 있고, 불법 네트워크 침입에 실시간으로 대응할 수 있으며, 네트워크 노드를 보안 정책에 의해 체계적으로 관리한다.
- <64> 상술한 바와 같은 본 발명의 방법은 프로그램으로 구현되어 컴퓨터로 읽을 수 있는 기록 매체(씨디롬, 램, 롬, 플로피 디스크, 하드 디스크, 광자기 디스크 등)에 저장될 수 있다. 이러한 과정은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있으므로 더 이상 상세히 설명하지 않기로 한다.

<65> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

【발명의 효과】

<66> 상기와 같이 본 발명은, 커널 내에서 침입탐지 과정에 이용되는 침입탐지규칙의 복사본을 동적으로 관리하여, 사용자(User) 영역으로부터 침입탐지규칙 변경 요청시, 상기 복사본에 대하여 변경 작업을 수행한 후, 현재 적용중인 침입탐지규칙과 교체(포인터 교환)함으로써, 침입탐지규칙의 변경시에도 침입탐지 과정의 연속성을 보장할 수 있는 효과가 있다.

<67> 또한, 본 발명은, 커널 내에 침입탐지규칙 변경 상태를 나타내기 위한 전역 변수를 할당하고, 상기 전역 변수를 이용하여 침입탐지규칙을 이용한 침입탐지 과정과 침입탐지규칙에 대한 변경 과정을 동시에 수행할 수 있으므로, 침입탐지규칙에 대한 일관성을 유지할 수 있는 효과가 있다.

【특허청구범위】**【청구항 1】**

커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법에 있어서,

커널 영역에서 침입탐지규칙의 복사본을 생성하는 제 1 단계;

사용자 영역으로부터의 침입탐지규칙의 변경 요청에 따라 상기 침입탐지규칙의 복사본을 변경하는 제 2 단계; 및

상기 침입탐지규칙을 가리키는 포인터의 값과 상기 변경된 침입탐지규칙의 복사본을 가리키는 포인터의 값을 서로 교환하여 현재 적용중인 침입탐지규칙을 변경하는 제 3 단계를 포함하는 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법.

【청구항 2】

제 1 항에 있어서,

상기 침입탐지규칙의 복사본을 현재 적용중인 침입탐지규칙과 동일하게 재변경하는 제 4 단계

를 더 포함하는 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법.

【청구항 3】

제 1 항 또는 제 2 항에 있어서,

상기 침입탐지규칙의 복사본을 변경하는 과정 및 침입탐지규칙을 변경하는 과정은,

미리 할당된 전역변수를 이용하여 커널 내의 침입탐지규칙 변경 상태를 나타내고, 상기 전역변수의 값에 따라 수행되는 것을 특징으로 하는 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법.

【청구항 4】

제 3 항에 있어서,

상기 커널 영역은,

상기 사용자 영역으로부터의 침입탐지규칙 변경 요청을 시스템 호출을 이용하여 전달하는 것을 특징으로 하는 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법.

【청구항 5】

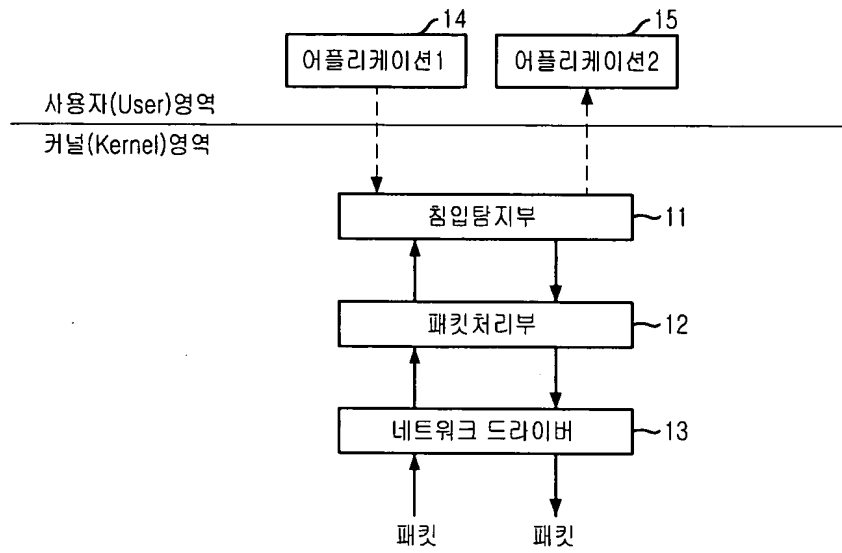
제 3 항에 있어서,

상기 커널 영역은,

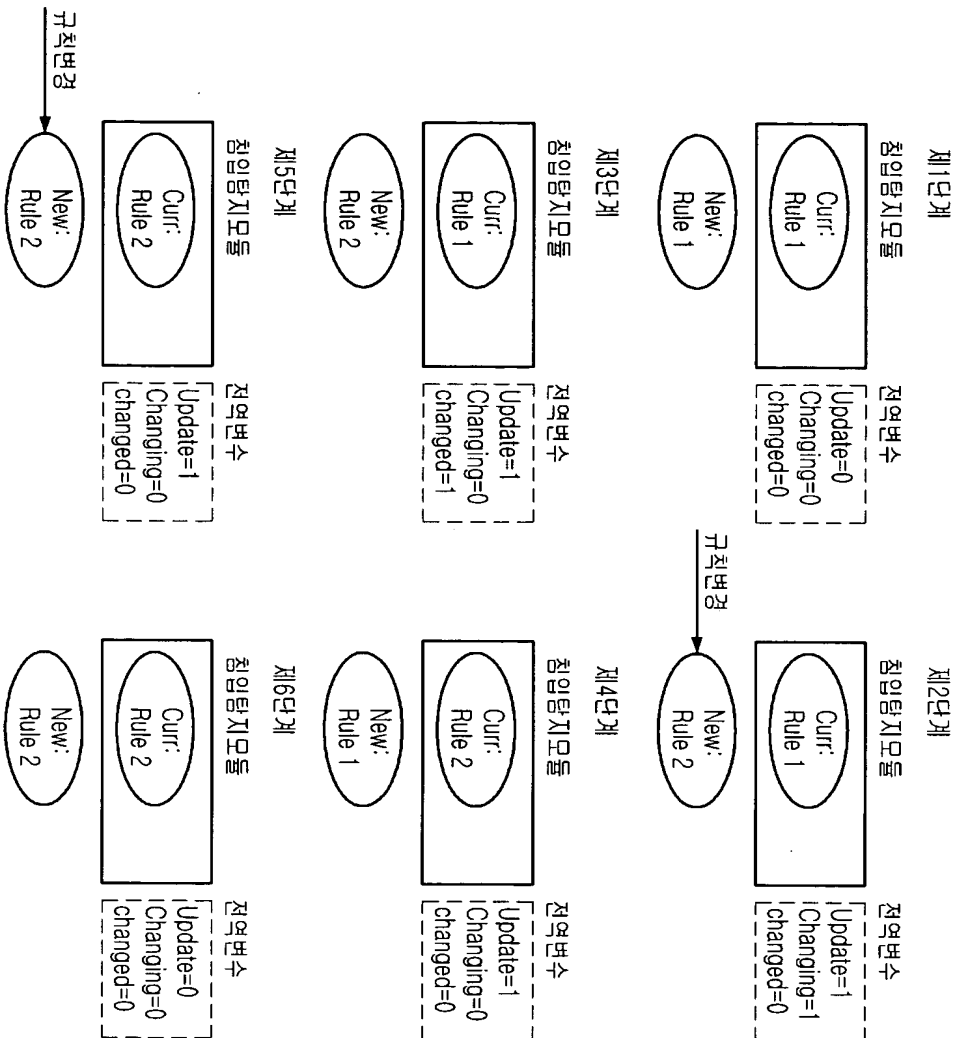
상기 침입탐지규칙을 적용한 침입탐지결과를 커널이 동작하는 호스트의 응용 프로그램 또는/및 외부 호스트 또는/및 외부 네트워크로 전달하되, 커널 내 전역 변수들을 설정하여 커널 내부에서 전달 장소를 판단하여 침입탐지결과를 전달하는 것을 특징으로 하는 커널 기반의 침입탐지시스템에서의 침입탐지규칙 동적 변경 방법.

【도면】

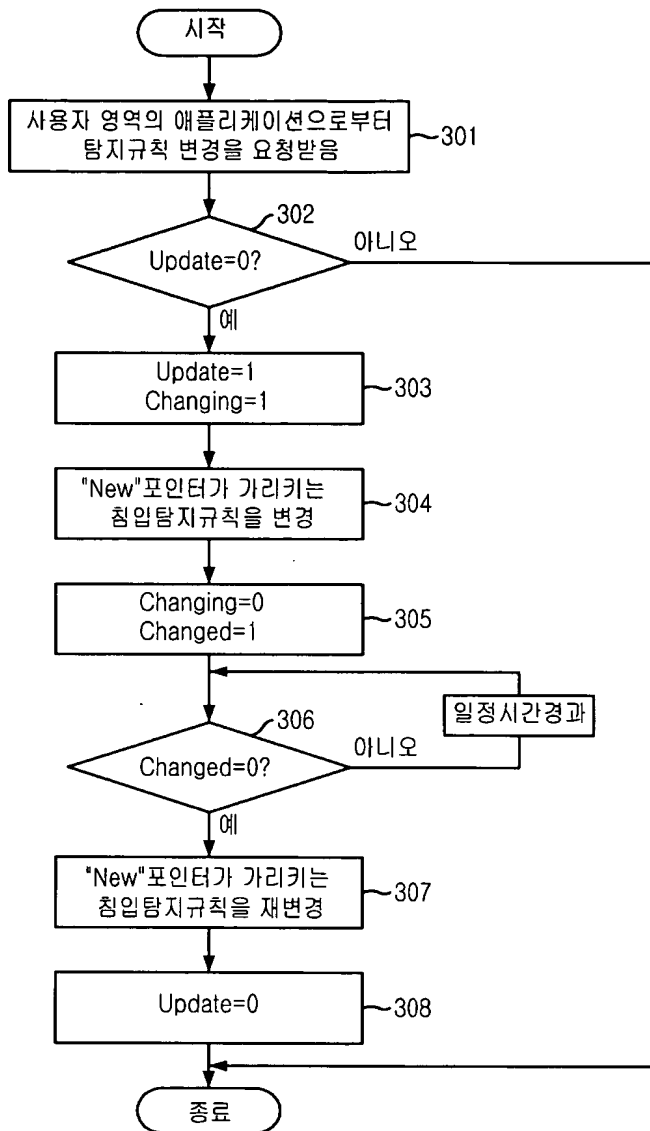
【도 1】



【도 2】



【도 3】



【도 4】

